Original article
UDC 343.98(510)
DOI 10.18101/2949-1657-2025-2-35-38

China's Influence on United Nations Cybercrime Legislation

© **Aleksandra V. Galdanova**
Master's Student,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
a_galdanova@mail.ru

Abstract. The article examines the growing influence of the People's Republic of China on the development of cybercrime legislation within the framework of the United Nations. It explores how China promotes the concept of "cyber sovereignty" and supports multilateral mechanisms that reflect its priorities in the fields of development and security. Special attention is given to China's participation in drafting the proposed UN Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes.
Keywords: China, UN, cybercrime, cyber sovereignty, international law, digital governance.

For citation
Galdanova A. V. China's Influence on United Nations Cybercrime Legislation. *Oriental Vector: History, Society, State.* 2025; 2: 35–38 (In Russ.)

The rapid rise of cybercrime as a transnational threat is prompting international institutions, especially the United Nations (UN), to develop mechanisms for global cooperation in this field. In this context, China has emerged as a key actor promoting an alternative vision of cyberspace governance—emphasizing state control, national security, and the principle of non-interference in internal affairs [4]. This article analyzes China's strategies for shaping international norms on combating cybercrime within the UN framework.

At the core of China's international cyber policy lies the principle of cyber sovereignty, which asserts the right of each state to control the internet within its own borders. Officially introduced at the World Internet Conference in Wuzhen in 2015, this concept sharply contrasts with the Western multistakeholder model based on openness, private sector involvement, and transparency [3]. China views cyberspace as an extension of physical sovereignty. It emphasizes the right of states to control ICT infrastructure, resources, data, and related activities within their territory—contrasting this with the Western model of cross-border access without consent [1].

China is actively promoting cyber sovereignty not only at national and regional levels, but also internationally—particularly at the UN, where it seeks recognition and legal codification of this approach [4].

The UN serves as a key platform for international dialogue on information security and cybercrime. These issues are considered within the UN Office on Drugs and Crime (UNODC) and the Third Committee of the UN General Assembly (Social, Humanitarian, and Cultural Issues). Until recently, the UN's efforts were limited to

adopting non-binding resolutions, including through the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) on information security.

A turning point came in 2019 with the adoption of resolution A/RES/74/247, supported by China and initiated by Russia. This resolution provides for the development of a comprehensive international convention on countering cybercrime.[1]

This step is seen as an alternative to the Council of Europe's 2001 Budapest Convention, which China has consistently opposed due to its principles of extraterritorial jurisdiction and lack of universal representation.[2]

China plays an active role in the work of the Ad Hoc Committee tasked with drafting the new convention. During the negotiations, China has proposed the following key provisions:

– Expansion of the scope of regulation: China proposes including not only traditional ICT-related crimes but also content-related offenses (e.g., "dissemination of false information" or incitement of hatred). This raises concerns among Western countries about potential restrictions on freedom of expression.[3]

– Data localization and access through state-to-state requests: China supports the requirement for state consent before cross-border access to digital evidence, reflecting the principle of sovereignty and a data localization policy.[4]

– Limiting extraterritoriality: China criticizes unilateral prosecutions of cybercriminals without international cooperation, particularly those carried out by the United States [4].

China's actions have elicited mixed reactions. Many Global South countries support the idea of a new convention that reflects their interests in digital sovereignty [3]. In contrast, OECD states and international human rights organizations express concern over the potential use of cyber legislation for authoritarian purposes.

Critics point to the risk of legitimizing repression under the guise of public security. China, in turn, insists on the need to protect national security and maintain social order [4].

China's legislative initiatives within the UN framework on cybercrime underscore its broader ambition to redefine the global digital order in alignment with its political philosophy, security concerns, and developmental goals. By promoting the concept of cyber sovereignty, China challenges the liberal, open, and decentralized model of internet governance traditionally advocated by Western states. Its emphasis on state

[1] United Nations General Assembly. Resolution A/RES/74/247 "Countering the use of information and communications technologies for criminal purposes" of 27 December 2019 // United Nations Documents. URL: https://undocs.org/A/RES/74/247 (accessed: 22.04.2025).

[2] United Nations Office on Drugs and Crime. Materials of the Ad Hoc Committee on Cybercrime, 2022–2024 // UNODC. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee (accessed: 22.04.2025).

[3] Ministry of Foreign Affairs of the People's Republic of China. China's Position on the UN Cybercrime Convention Negotiations. 2022. URL: https://www.fmprc.gov.cn (accessed: 22.04.2025).

[4] United Nations Office on Drugs and Crime. Materials of the Ad Hoc Committee on Cybercrime, 2022–2024 // UNODC. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee (accessed: 22.04.2025).

control, national jurisdiction, and the protection of public order presents a fundamentally different vision of international cyber cooperation.

The ongoing negotiations on the new UN cybercrime convention have become a critical platform where competing global visions of internet governance are contested. On one side, China and several Global South countries advocate for a model that prioritizes sovereignty, data localization, and content regulation, arguing that such measures are essential for national stability, security, and development. On the other, Western democracies stress the importance of safeguarding human rights, especially freedom of expression and privacy, fearing that vague legal definitions and expanded state powers could legitimize digital authoritarianism.

This polarization presents both challenges and opportunities. On the one hand, the divergence of approaches risks slowing down the consensus-building process and leading to parallel or fragmented legal regimes. On the other, it opens the door for broader participation of developing countries in shaping international norms, offering a chance to create more inclusive and representative frameworks.

Finding common ground will require sustained diplomatic engagement, mutual recognition of different national contexts, and a balanced approach that reconciles legitimate concerns over national security with the protection of fundamental rights. As China continues to assert itself as a norm entrepreneur in the digital domain, its influence will likely remain a defining factor in the evolution of international cyber governance.

Ultimately, the outcome of the UN cybercrime convention will not only determine the legal tools available for combating cyber threats but also set precedents for how the internet is governed globally—whether as a space of state-centric control or as a borderless domain of shared responsibility. The challenge for the international community lies in crafting a treaty that is both effective and equitable, capable of bridging ideological divides while addressing the pressing realities of global cybercrime.

References

1. Arun S., Arindrajit B. Back to the Territorial State: China and Russia's Use of UN Cybercrime Negotiations to Challenge the Liberal Cyber Order. *Journal of Cyber Policy.* 2024; 9 (2): 256–287. URL: https://doi.org/10.1080/23738871.2024.2436591 (accessed: 23.04.2025).

2. Broeders D., Berg B. Governing Cyberspace: Behaviour, Power and Diplomacy. London, Rowman & Littlefield International. 2020. 337 p. Available at: https://rowman.com/WebDocs/Open_Access_Governing_Cyberspace_Broeders_and_van_den_Berg.pdf (accessed: 23.04.2025).

3. Lewis J. A. China's Information Controls, Global Media Influence, and Cyber Warfare Strategy. Center for Strategic and International Studies, 2017, 9 p. Available at: https://www.csis.org/james-lewis-publications (accessed: 22.04.2025).

The article was submitted 20.09.2025; approved after review 22.09.2025; accepted for publication 08.10.2025.

Влияние Китая на законодательство ООН о киберпреступности

Александра В. Галданова
магистрант,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
a_galdanova@mail.ru

Аннотация. В статье рассматривается растущее влияние Китайской Народной Республики на развитие законодательства о киберпреступности в рамках Организации Объединенных Наций. Рассматривается продвижение Китаем концепции «киберсуверенитета» и поддержка многосторонних механизмов, отражающих его приоритеты в области развития и безопасности. Особое внимание уделяется участию Китая в разработке проекта Конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях.
Ключевые слова: Китай, ООН, киберпреступность, киберсуверенитет, международное право, цифровое управление.

Для цитирования
Галданова А. В. Влияние Китая на законодательство ООН о киберпреступности // Восточный вектор: история, общество, государство. 2025. Вып. 2. С. 35–38.

Статья поступила в редакцию 20.09.2025; одобрена после рецензирования 22.09.2025; принята к публикации 08.10.2025.